REMARKS

Claims 1-36 were pending after submission of the Request for Continued Examination filed August 18, 2004. Claim 5 is amended. Claims 37-51 are new. No new matter has been added. The Applicant respectfully requests that the Examiner consider the foregoing comments prior to issuing a new action or notice.

Substance of the Interview

Applicant thanks Examiner Elisca for extending the courtesy of an interview on September 27, 2004, which was attended by Applicant's attorneys Jennifer Zanocco and Mark Kirkland and Examiner Elisca. At the interview, the attendees discussed the claims, U.S. Patent Number 6,549,626 (Al-Salqan) and the anti-spoofing protection techniques afforded by the claimed invention. No amendments or change in status of the claims was agreed to during the interview.

Additional Claims

The foregoing comments further the response of August 18, 2004. The remarks and description of Al-Salqan as found in the response of August 18, 2004, are included herein by reference.

Claim 37 depends from claim 36. Claim 37 recites a method including steps performed at the sender, at the intended recipient and at the third party. The sender encrypts a symmetric key with a public key of the third party. The sender sends the encrypted symmetric key to the intended recipient. The intended recipient cannot access the symmetric key or the message prior to the intended recipient returning a signed receipt to the third party. The signed receipt includes a hash of the encrypted message.

Al-Salqan describes a method of storing a password so that the password can be recovered in the event the password is lost (Abstract, lines 1-3). A principal encodes private information of the principal (column 2, lines 50-52). The encoded result is used to encrypt the password to be stored (column 2, lines 52-54). The encrypted password is again encrypted,

using the public key of a trusted party, thereby creating a key recovery file (column 2, lines 54-59). The key recovery file is stored by the trusted party (column 5, lines 46-58). Later, when the principal wants to recover the password, the principal sends the private information to the trusted party (column 5, lines 36-45). The trusted party compares the received private information with stored private information (column 5, lines 59-67). Upon determining the private information received is that of the principal, the trusted party retrieves the key to send to the principal (*id.*).

In Al-Salqan, the principal has to prove that the principal is the proper party to send the password to. The principal proves that the principal is indeed the principal by providing the private information. The principal and trusted party have access to the private information at all times. Conversely, claim 37 requires that the intended recipient cannot access the symmetric key or the message prior to returning a signed receipt to the third party. Claim 37 provides a sender with a way to ensure that a recipient cannot access a message without first sending a receipt for the message. In Al-Salqan, the private information and the password are not kept from the principal or the trusted party.

Claim 37 also requires that the receipt includes a hash of the encrypted message. In Al-Salqan, neither the trusted party nor the principal sign a receipt that is tied to a message or return a signed hash of an encrypted message to another party. Rather, the principal accesses the password by sending the trusted party the private information. The private information is not tied to the password the way a hash of an encrypted message is tied to the message. Further, the principal does not send a hash of information that the principal cannot access. For at least the above stated reasons, Al-Salqan does not suggest or teach a sender encrypting a symmetric key and sending the encrypted symmetric key so that a recipient cannot access the symmetric key or message prior to the recipient returning a signed receipt to a third party.

Claim 37 additionally includes a step performed at the recipient. The recipient returns a signed receipt to the third party. Returning the signed receipt includes sending a hash of the encrypted content in the message and sending the encrypted symmetric key, but not sending the encrypted content to the third party.

Al-Salqan transfers an encrypted encoded file between a principal and a trusted party. The trusted party receives the encrypted encoded file and the private information used to encode

a key. The trusted party therefore has access to the private information, the key and the trusted party's asymmetric keys. Therefore, there is no content that is withheld from the trusted party or the principal. Conversely, the method described in claim 37 does not provide the message content, in either encrypted or non-encrypted form, to the third party. Al-Salqan does not teach or suggest sending a hash of encrypted content in a message and sending an encrypted symmetric key, but not the encrypted content to a third party.

Claim 37 further includes a series of steps performed at the third party. The third party verifies that a first hash of the encrypted content equals a second hash of the encrypted content. The first hash is created by the sender and the second hash is created by the recipient. The third party transfers a verified receipt to a sender and provides the symmetric key to the intended recipient. A signed receipt from the recipient includes the second hash.

Al-Salqan describes a trusted party that acts as a repository for keys, but does not verify that a recipient receives an encrypted message or that a sender sent message content that the sender receives a receipt for having sent. The trusted party compares private information provided by the principal to the private information received from the principal at an earlier stage in the storage process. Al-Salqan does not verify that a first hash of encrypted content equals a second hash of encrypted content. Thus, Al-Salqan does not teach or suggest verifying that a first hash of the encrypted content sent by a sender equals a second hash of the encrypted content sent by an intended recipient.

Further, in Al-Salqan, the principal and the trusted party exchange information. The principal sends the encrypted encoded file to the trusted party and the trusted party sends the key back to the principal. However, the trusted party does not send information to an additional party along with sending the key back to the principal. Thus, Al-Salqan does not teach or suggest transferring a verified receipt to a sender with providing a symmetric key to an intended recipient.

Claim 37 requires that a first hash of the encrypted content and a second hash of the encrypted content are equal. The third party sends a receipt that includes the second hash, which is signed by the intended recipient, showing the intended recipient received the encrypted

message. The third party can verify that the message is the same message for which a receipt was provided for by the recipient. This prevents spoofing by either the sender or the recipient.

For at least the reasons provided above, Applicant submits that claim 37 is not anticipated by Al-Salqan. For at least this reason, in addition to the reasons provided in the response of August 18, 2004, Applicant submits that claim 37 is not anticipated.

Claim 44 depends from claim 4. Claim 44 recites a method that includes verifying a signed receipt to ensure that an intended recipient received an encrypted message sent by the sender. The signed receipt memorializes receipt of an encrypted message by the intended recipient.

Al-Salqan verifies that the principal, or another party with access to the principal's information, is the proper recipient for the stored password. Al-Salqan does not describe determining whether a party received a message. Both the trusted party and the principal fail to send a receipt that memorializes receipt of an encrypted message. Neither receive a signed receipt or verify a signed receipt. Therefore, Al-Salqan does not teach or suggest verifying a signed receipt to ensure that a recipient received an encrypted message sent by a sender. For at least these reasons, Applicant submits that claim 44 is not anticipated.

Claim 46 depends from claim 6. Claim 46 recites a method including forwarding a symmetric key to an intended recipient after verifying a certified receipt. The certified receipt is verified by a third party and indicates receipt of a message by the intended recipient.

As described above, Al-Salqan is a repository for keys or passwords that are lost. Al-Salqan does not address determining whether a party receives a message. The third party does not receive (or send) a receipt for a message and therefore does not verify a certified receipt. Although the trusted party forwards a password, the password is forwarded after the trusted party determines that the principal, or another party, has sent the correct private information to the trusted party. The private information is not a certified receipt that indicates receipt for a message. Al-Salqan does not suggest or disclose forwarding a symmetric key to an intended recipient after verifying a certified receipt. For at least this reason, Applicant submits that claim 46 is not anticipated by Al-Salqan.

Claim 47 depends from claim 7. Claim 47 recites a method including forwarding an encrypted symmetric key to a third party. The symmetric key is used to encrypt a message from a sender. The message is not exposed to the third party.

Al-Salqan describes a trusted party and a principal who both start out with access to the password sent to the trusted party for storage, and the private information that is encoded and used to encrypt the password. The trusted party must have access to the private information to compare the private information sent by the principal at the time of storing the password to the private information received at the time the principal wants to access the password again. The principal must have access to the private information to retrieve the stored password. The trusted party can decrypt the password at any time, because the trusted party has its own private key, the private information and the stored password. The principal may lose the password at some point, but the principal has the password at the time of storing the password for storage. The password is never kept from the principal at any time.

Al-Salqan fails to suggest or disclose forwarding an encrypted symmetric key to a third party, but not exposing a message encrypted with the symmetric key to the third party. For at least this reason, Applicant submits that claim 47 is not anticipated by Al-Salqan.

Claim 49 depends from claim 8. Claim 49 recites a method including receiving a first hash of an encrypted message from a sender. The encrypted message is also received from the sender. The received encrypted message is hashed to form a second hash of the encrypted message. The first and second hashes are sent to a third party to verify that the first hash equals the second hash.

If the first hash and the second hash are equal, what the sender is sending as the encrypted message and what the recipient has received as an encrypted message are the same. Al-Salqan does not determine whether a message that a party purports to have sent is the same as a message that another party has received. Al-Salqan only suggests that a hashing function can be used to encode personal information to use as a symmetric key. Al-Salqan does not suggest creating two hashed inputs created by two different parties. Al-Salqan does not suggest or disclose receiving a first hash of an encrypted message, hashing an encrypted message to form a second hash of the encrypted message, and sending the two hashes to a third party to verify that

the first hash equals the second hash. For at least this reason, Applicant submits that claim 49 is not anticipated by Al-Salqan.

As discussed in the remarks in the response of August 18, 2004, Al-Salqan does not describe a receipt including a representation of the encrypted message. As discussed above, because the recipient signs the receipt, the signed receipt can be used to show that an encrypted message has been received by the recipient. Al-Salqan is directed at storing passwords and keys for future access, rather than proving that a recipient has received an encrypted message. Further, while the trusted party sends a key or password to the principal, the trusted party does not transfer a receipt to a sender. Thus, the trusted party does not also transfer a receipt that includes a representation of an encrypted message to a party other than the principal. In short, Al-Salqan does not suggest or disclose a receipt including a representation of an encrypted message, Al-Salqan does not suggest or disclose a third party transferring a receipt to a sender and Al-Salqan does not suggest or disclose a recipient signing a receipt. For these additional reasons, Applicant submits that claim 1 is not anticipated by Al-Salqan, along with other independent claims that are pending in the instant application that include similar limitations.

Applicant asks that all claims be examined in view of the amendment to the claims.

Please apply excess claims fees of $135.00 and any other appropriate charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 9/29/04

Jennifer A. Zahocco
Reg. No. 54,563

Customer No.: 26181
Fish & Richardson P.C.
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

50239257.doc